KESGRAVE TOWN COUNCIL

Data Protection Policy (Use of CCTV)

1. Background

1.1 Council uses closed circuit television (CCTV) images for the prevention, identification and reduction of crime and monitoring of its property in order to provide a safe and secure environment for staff and residents and to prevent the loss or damage to Council property.

1.2 CCTV surveillance is intended for the purposes of:

- protecting Council's assets;
- promoting the health and safety of staff and residents;
- reducing the incidence of crime and anti-social behaviour (including vandalism);
- supporting the Police in a bid to deter and detect crime; and
- assisting in identifying, apprehending and prosecuting offenders.

1.3 The system comprises of 4 fixed cameras positioned at the Multi-Use Games Area located at Cedarwalk Green, Kesgrave (the "MUGA").

1.4 The CCTV system is owned and operated by Council and the deployment of which is determined by Council through the Clerk.

1.5 The CCTV is not continuously monitored. Data/images are accessed upon receipt of reports of potential criminal or anti-social behaviour.

1.6 The CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act. This Policy outlines Council's use of CCTV and how it complies with the Act.

1.7 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained in their responsibilities under the Information Commissioner's Office (ICO) CCTV Code of Practice appended to this policy. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

1.8 Council complies with the ICO CCTV Code of Practice appended to this policy to ensure its CCTV system is used responsibly and safeguards both trust and confidence in its continued use.

1.9 The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this Policy e.g. CCTV will not be used for monitoring employee performance.

1.10 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by Council, including its Complaints Policy and Procedure.

2. Justification for Use of CCTV

The use of CCTV to monitor the MUGA for security purposes has been deemed to be justified by Council. The system is intended to capture images of individuals damaging or misusing property or any anti-social behaviour within or close to the MUGA.

3. Data Protection Impact Assessments

Where new CCTV systems or cameras are to be installed, Council will carry out a full Data Protection Impact Assessment identifying risks related to the installation and ensuring full compliance with data protection legislation. This may involve the need for consultation with staff and local residents.

4. Location of Cameras

4.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.

4.2 Council will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

4.3 CCTV will not be used within Council premises.

4.4 Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by.

4.5 CCTV Video Monitoring and Recording of Public Areas may include the following:

- protection of Council property: building perimeters, entrances and exits; and
- criminal investigations (carried out by the Police): robbery, burglary and theft surveillance.

5. Covert Surveillance

Council will not engage in covert surveillance.

6. Notification

6.1 A copy of this CCTV Policy will be provided on request to staff or residents and will be made available on Council's website.

6.2 The location of CCTV cameras will also be indicated and adequate signage will be placed at each location in which a CCTV camera is sited to indicate that CCTV is in operation. Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, gates; and
- at or close to each camera.

7. Storage and Retention

7.1 The images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue and will be destroyed within six months of its final conclusion.

7.2 The images/recordings will be stored in a secure environment with a log of access kept.

7.3 Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Clerk. The Clerk may delegate the administration of the CCTV System to another staff member.

7.4 In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

8. Access

8.1 Recorded data/images will be securely stored in a restricted place. Unauthorised access will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access will be maintained.

8.2 Access to the CCTV system and stored images will be restricted to authorised personnel only.

8.3 A record of the date of any disclosure request along with details of who the information has been provided to (the name of the person and the organisation they represent), why they required it and how the request was dealt with will be made and kept, in case of challenge.

8.4 Data will be provided to those requests authorised in a permanent format where possible. If this is not possible the data subject will be offered the opportunity to view the footage.

8.5 In relevant circumstances, CCTV footage may be accessed by any of the following:

- by the police where Council is required by law to make a report regarding the commission of a suspected crime;
- following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on or near Council property;
- by the HSE and/or any other statutory body charged with child safeguarding; or
- by data subjects (or their legal representatives), pursuant to a Subject Access Request;
- by individuals (or their legal representatives) subject to a court order; and
- by Council's insurance company where it requires same in order for Council to pursue a claim for damage done to the insured property.

9. Subject Access Requests (SAR)

9.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

9.2 Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified, for example, date, time and location.

9.3 Council will respond to requests within 30 calendar days of receipt in accordance with the Individual Rights specified in Council's Data Protection Policy (General).

9.4 Council reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

9.5 A record of the date of the disclosure along with details of whom the information has been provided (the name of the person and where applicable the organisation they represent), and why they required it, will be made.

9.6 In giving a person a copy of their data, Council will provide a still/series of still pictures and/or an electronic form of the relevant images. However, other images of other individuals will be obscured before the data is released.

10. Complaints

Complaints about the operation of CCTV will be dealt with in accordance with Council's Complaints Policy and Procedure which is available on its website.

11. Staff Training

11.1 Staff authorised to access the CCTV system will be trained to comply with this Policy. Staff will understand that all information relating to the CCTV images must be handled securely.

11.2 Staff will receive appropriate training to enable them to identify and handle different requests according to regulations.

11.3 Staff misuse of surveillance system information will lead to disciplinary proceedings.

12. Responsibilities

12.1 The Clerk (or nominated staff member) will:

- ensure that the use of CCTV systems is implemented in accordance with this Policy;
- oversee and co-ordinate the use of CCTV monitoring for safety and security purposes;
- ensure that all existing CCTV monitoring systems are evaluated for compliance with this Policy;

- ensure that Council's CCTV monitoring is consistent with the highest standards and protections;
- review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this Policy;
- maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system;
- ensure that the perimeter of view from fixed location cameras conforms to this Policy;
- give consideration to residents' complaints, if any, regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment;
- ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals and be mindful that no such infringement is likely to take place;
- ensure that cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy";
- ensure that monitoring footage are stored in a secure place with access by authorised personnel only;
- ensure that images recorded are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil);
- ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy;
- ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics; and
- ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

Policy effective from: 26 June 2023

Date for next review: 26 June 2025 (or earlier if relevant legislation changes before this date)